Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie BSI TR-03116-1

Kryptographische Vorgaben für Projekte der Bundesregierung

Teil 1: Telematikinfrastruktur

Version:	3.20
Datum:	21.09.2018
Autoren:	Technische Arbeitsgruppe TR-03116-1
Status:	Veröffentlichung
Fassung:	September 2018

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-111
E-Mail: zertifizierung@bsi.bund.de
Internet: http://www.bsi.bund.de

Vorwort

Die Technische Richtlinie BSI TR-03116 stellt eine Vorgabe für Projekte der Bundesregierung dar. Die Technische Richtlinie ist in fünf Teile gegliedert:

- Der vorliegende Teil 1 der Technischen Richtlinie legt die im Gesundheitswesen verbindlichen Sicherheitsanforderungen und –vorgaben für den Einsatz kryptographischer Verfahren für die elektronische Gesundheitskarte (eGK), den Heilberufsausweis (HBA) und die technischen Komponenten der Telematikinfrastruktur fest.
- Teil 2 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in hoheitlichen Ausweisdokumenten [TR-03116-2].
- Teil 3 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren für die Infrastruktur von intelligenten Messsystemen im Energiesektor [TR-03116-3].
- Teil 4 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für die Verwendung von SSL/TLS, S/MIME und OpenPGP in eGovernment-Anwendungen [TR-03116-4].
- Teil 5 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in Anwendungen der Secure Element API (wie Technischen Sicherheitseinrichtungen elektronischer Aufzeichnungssysteme) [TR-03116-5].

1 Zielstellung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt mit dieser Technischen Richtlinie eine Bewertung der Sicherheit und eine langfristige Orientierung für den Einsatz kryptographischer Verfahren der elektronischen Gesundheitskarte, des Heilberufsausweises, der technischen Komponenten und der Dienste der Telematikinfrastruktur des Gesundheitswesens.

Diese Technische Richtlinie richtet sich an die gematik, die Hersteller von technischen Komponenten, die Herausgeber von elektronischen Gesundheitskarten (eGK), Heilberufsausweisen (HBA) und Secure Module Cards (SMC) und die Anbieter von Diensten und Anwendungen in der Telematikinfrastruktur. Sie ist verbindlich bei der Auswahl der kryptographischen Algorithmen.

Die in dieser Technischen Richtlinie betrachteten kryptographischen Verfahren wurden unter Berücksichtigung ihrer Sicherheit und Vertrauenswürdigkeit und des gegenwärtigen Standes der Spezifikationen ausgewählt. Für die genaue Spezifikation der kryptographischen Verfahren wird auf die einschlägige Literatur verwiesen.

Dieses Dokument soll in Übereinstimmung mit der weiteren Entwicklung des Einsatzgebietes, der kryptologischen Forschung und der Erfahrungen mit praktischen Realisierungen jährlich durch das BSI aktualisiert und bei Bedarf ergänzt werden.

Kapitel 2 beschreibt die Sicherheitsziele und die Grundsätze zur Bewertung des Einsatzes kryptographischer Verfahren im Gesundheitswesen.

In Kapitel 3 wird die **grundsätzliche Eignung von Algorithmen bzw. Sicherheitsverfahren** – unabhängig von der konkreten Applikation sowie Einsatzumgebung bzw. Anwendung in Komponenten in der Telematik im Gesundheitswesen – gegeben. Hierzu werden die Angaben anhand des vorgesehenen Sicherheitsmechanismus gegliedert. Dadurch kann ein spezifischer Algorithmus (z.B. AES) auch mehrfach genannt werden, sofern der Algorithmus für die Anwendung in verschiedenen Sicherheitsmechanismen (z.B. Authentisierung von Komponenten, Datenverschlüsselung und Schlüsselverwaltung) als geeignet bewertet wird.

Zu den in Kapitel 3 grundsätzlich als geeignet bewerteten kryptographischen Verfahren werden in Kapitel 4 **Empfehlungen zum Einsatz kryptographischer Verfahren für eine spezifische Anwendungen bzw. Einsatzumgebung** gegeben.

Generell enthält diese Technische Richtlinie nur Aussagen über die Eignung kryptographischer Verfahren bis Ende 2024. Abgesehen von unvorhergesehenen kryptographischen Durchbrüchen, die nicht vollkommen ausgeschlossen werden können aber unwahrscheinlich sind, lassen sich über einen Zeitraum von ca. 7 Jahren relativ verlässliche Aussagen machen. Ist eine weitere Verwendung des Verfahrens über diesen Zeitraum hinaus aus heutiger Sicht nicht ausgeschlossen, so wird dies mit 2024+ gekennzeichnet.

In dieser Technischen Richtlinie geht es um Aussagen zur Sicherheit von kryptographischen Algorithmen. Die Aussage „es wird die Verwendung von Algorithmus X empfohlen“ ist so zu verstehen, dass der Algorithmus X das in der vorliegenden technischen Richtlinie ange-

strebte Sicherheitsniveau erreicht. Dabei kann es durchaus vorkommen, dass manche empfohlenen Algorithmen ein höheres Sicherheitsniveau aufweisen als andere: zum Beispiel ist SHA-512 gegen heute absehbare Angriffe sicherer als SHA-256. Es kann auch vorkommen, dass in dieser Technischen Richtlinie nicht empfohlene kryptographische Algorithmen tatsächlich kryptographisch stark sind. Insgesamt werden nur gut untersuchte und für den praktischen Einsatz relevante Verfahren empfohlen, die gegen alle für den Vorhersagezeitraum als relevant eingeschätzten kryptoanalytischen Angriffsvektoren sicher sind.

Die langfristige Vertraulichkeit verschlüsselter Daten wirft grundsätzliche Probleme auf. Bei Verwendung der bis Ende 2024 als generell, d.h. ohne Beschränkung auf spezielle Anwendungen geeignet eingestuften und empfohlenen Verfahren zur Schlüsselvereinbarung und zur symmetrischen bzw. asymmetrischen Verschlüsselung (z. B. für Schlüsselaustausch) dürfte die Vertraulichkeit der verschlüsselten Daten nach Einschätzung des BSI im Zeitraum von ca. 10 Jahren (bis Ende 2028) noch ausreichend gesichert sein. Diese Einschätzung ist allerdings schon mit einem höheren Maß an Spekulation verbunden als die Aussagen über 7 Jahre und daher weniger belastbar. Aussagen zur Sicherheit über mehr als ein Jahrzehnt sind dagegen kaum möglich.

Da ein Angreifer die über das Internet übertragenen Daten langfristig speichern kann, um sie später zu entschlüsseln, kann ein ***langfristiger Schutz solcher Daten grundsätzlich nicht garantiert*** *werden.*

Daraus ergeben sich folgende Konsequenzen:

- Die über das Internet übertragene vertrauliche Information ist auf das notwendige Maß zu beschränken.
- Die Infrastruktur muss für einen Übergang auf stärkere kryptographische Verfahren ausgelegt sein. Insbesondere sind (z.B. auf Servern) gespeicherte vertrauliche Daten bei einem solchen Übergang neu zu verschlüsseln und die alten Datensätze zu löschen.

Bemerkung zu der Hashfunktion SHA-1: Die Kollisionsangriffe der Arbeitsgruppe um die chinesische Kryptologin X. Wang haben eine dynamische Entwicklung bei der kryptographischen Analyse von Hashfunktionen ausgelöst (vgl. bspw. [Stevens-2017]). Daher muss die weitere Entwicklung bei der Hashfunktion SHA-1 im Auge behalten werden; alle Aussagen dieses Papiers hierzu sind als vorläufig zu betrachten und können sich im Rahmen der vorgesehenen jährlichen Anpassung (oder einer Anpassung bei Bedarf) der technischen Richtlinie ändern.

2 Grundsätze

2.1 Sicherheitsziele für den Einsatz kryptographischer Verfahren im Gesundheitswesen

Der Einsatz kryptographischer Verfahren im Gesundheitswesen erfolgt mit den folgenden übergreifenden Sicherheitszielen:

1. Die kryptographischen Verfahren sollen die Vertraulichkeit personenbezogener insbesondere medizinischer Daten bei deren Übertragung und während ihrer Speicherung in technischen Systemen der Telematikinfrastruktur des Gesundheitswesens auch langfristig sichern.
2. Die kryptographischen Verfahren sollen die Authentizität und Verbindlichkeit insbesondere personenbezogener Verordnungen, medizinischer Daten und anderer Dokumente durch qualifizierte elektronische Signatur und in gesondert ausgewiesenen Anwendungsbereichen durch fortgeschrittene Signatur bei vergleichbarer kryptographischer Sicherheit gewährleisten.
3. Die kryptographischen Verfahren sollen die sichere Authentisierung der Kommunikationspartner als Voraussetzung für die Zugriffskontrolle auf die Ressourcen der Telematikinfrastruktur sowie den Schutz der Vertraulichkeit und Integrität der Kommunikation technischer Komponenten unabhängig von den oben genannten Sicherheitsanforderungen gewährleisten.

Bemerkung: Das Sicherheitsziel der Verfügbarkeit der technischen Komponenten sowie die Sicherung der Systeme wie Primärsysteme, die zum Zugriff auf die Klardaten autorisiert sind, stehen außerhalb der Betrachtung dieser TR.

Die kryptographischen Verfahren sollen durch nachgewiesen vertrauenswürdige technische Komponenten implementiert werden. Die Vertrauenswürdigkeit der technischen Komponenten soll jeweils dem vorgesehenen Einsatzzweck angemessen durch Common Criteria Zertifikate, ergänzende Verfahren des BSI oder andere Sicherheitsgutachten nachgewiesen werden.

Mit den Sicherheitsvorgaben dieser Technischen Richtlinie wird ein Sicherheitsniveau von mindestens 100 Bit angestrebt. Anwendungsspezifische Ausnahmen müssen begründet werden. Bis Ende 2023 wird das Erreichen eines Sicherheitsniveaus von mindestens 120 Bit angestrebt. Danach ist das Sicherheitsniveau von 120 Bit verpflichtend. Damit wird einerseits ein angemessenes Sicherheitspolster gegenüber Fortschritten in der Kryptoanalyse und in der Rechentechnik geschaffen, wie es für eine Fortschreibung der in den letzten Jahren üblichen 7-Jahres-Prognosen benötigt wird. Andererseits wird hiermit ein ähnliches Sicherheitsniveau in allen als geeignet angesehenen Signaturverfahren erreicht; in den Vorjahren war der Sicherheitsspielraum der auf elliptischen Kurven basierenden Verfahren etwas größer als bei den Verfahren, die auf dem RSA-Problem oder dem Problem der Berechnung diskreter Logarithmen in endlichen Körpern beruhen. Zudem erfolgt auf diesem Wege eine Angleichung des Sicherheitsniveaus an internationale Vorgaben mit vergleichbarer inhaltlicher Grundausrichtung wie etwa den SOGIS-Kryptokatalog [SOGIS-2018] oder internationalen und nationalen Empfehlungen [ENISA-2014, TR-02102-1]. Dafür müssen bis spätestens Ende 2023 Teile der PKI, der Komponenten und der Dienste der TI verändert werden. Die erste Phase dieser Migration ist aktuell in der Umsetzung (Objektsysteme der Kartengeneration 2.1 und entsprechende PKI).

2.2 Grundsätze der Sicherheitsbewertung

Die Sicherheitsbewertung der kryptographischen Verfahren erfolgt auf dem gegenwärtigen Stand kryptographischer Erkenntnisse in Übereinstimmung mit den Sicherheitserfordernissen und unter Berücksichtigung der Einsatzbedingungen der elektronischen Gesundheitskarte, des Heilberufsausweises und technischer Komponenten der Telematikinfrastruktur des Gesundheitswesens. Die in diesem Dokument getroffenen Sicherheitsbewertungen kryptographischer Verfahren sind an die beschriebenen Einsatzbereiche gebunden. Ebenfalls wird vorausgesetzt, dass die Implementierungen und Hintergrundsysteme (wie z.B. die eingesetzten PKIs) dem Stand der kryptographischen Forschung entsprechen und korrekt arbeiten.

Die Sicherheitsbegutachtung der Produkte soll die Implementierung kryptographischer Verfahren einschließen. Die notwendige Vertrauenswürdigkeit kann aber im Rahmen der Produktevaluierung nur für solche kryptographischen Verfahren erreicht werden, zu denen bereits ausreichend gesicherte kryptographische Erkenntnisse vorliegen. Dieses Dokument unterstützt die Evaluierung und Zertifizierung der technischen Komponenten als Referenz auf sichere kryptographische Verfahren, da deren Bewertung nicht innerhalb der Produktevaluierung geleistet werden kann.

Für eine langfristige Planungssicherheit der Spezifikation, Entwicklung, Produktion und Anwendung der Produkte werden Empfehlungen zur weiteren Entwicklung der kryptographischen Verfahren gegeben. Die Orientierung an den Prognosen muss mit der kontinuierlichen Überwachung der Systemsicherheit und der Vorbereitung fallbezogener Maßnahmen zum Erhalt und ggf. zur Wiederherstellung der Systemsicherheit verbunden sein.

Es ist vorgesehen, die in diesem Dokument getroffenen Bewertungen und Orientierungen regelmäßig zu überprüfen.

3 Kryptographische Algorithmen und Parameter

In diesem Kapitel werden zunächst Vorgaben und Empfehlungen zu einigen speziellen kryptographischen Algorithmen gemacht, um darauf aufbauend die folgenden Sicherheitsmechanismen zu betrachten:

- Instanzauthentisierung (Gegenseitige Authentisierung von Komponenten) mit bzw. ohne Schlüsselvereinbarung,
- Datenauthentisierung (Message Authentication Code, Hashfunktionen, Signaturverfahren),
- Verschlüsselung,
- Erzeugung von Zufallszahlen und
- Schlüsselerzeugung.

Zu den einzelnen Algorithmen bzw. Sicherheitsmechanismen werden relevante internationale Standards angegeben.

3.1 Hashfunktionen

Für den Einsatz in der TI sind folgende Hashfunktionen bis Ende 2024+ zulässig:

- SHA-256, SHA-512/256, SHA-384, SHA-512 [FIPS-180-4]
- SHA3-256, SHA3-384, SHA3-512 [FIPS-202]

Für bestimmte Einsatzzwecke wie HMAC oder Schlüsselableitungen ist SHA-1 [FIPS-180-4] bis auf weiteres zulässig (vgl. Abschnitt 3.6.1).

Aktuell verwenden fast alle Komponenten und Dienste der TI, die TLS verwenden, TLS in der Version 1.2. Innerhalb von TLS Version 1.1 wird als PRF eine Konstruktion aus SHA-1 und MD5 verwendet[1]. Die Verwendung dieser PRF ist bis auf weiteres bei ausgewählten Bestandssystemen und Komponenten zulässig. Die Verwendung von TLS Version 1.1 wird perspektivisch unzulässig, insbesondere auch aufgrund der Verwendung von SHA-1 innerhalb von Signaturen[2].

3.2 RSA

Für die RSA-Verfahren nach [PKCS#1] und [ISO-9796-2] müssen zwei Primzahlen p und q zufällig (vgl. Abschnitt 3.9) und unabhängig voneinander erzeugt werden, mit n=p*q. Die beiden Zahlen p und q sollten nicht zu dicht aneinander und nicht zu weit voneinander entfernt liegen. Es soll gelten

$$|p-q| \geq 2^{n/2-100}$$

In [TR-02102-1, Abschnitt B.5] werden Verfahren für die Erzeugung von Primzahlen aufgeführt, die dies sicherstellen.

Bei der Verwendung probabilistischer Primzahltests zur Erzeugung von p und q darf die Wahrscheinlichkeit, dass die Zahlen doch keine Primzahlen sind, höchstens 2^{-100} betragen.

Bis Ende 2023 sind Schlüssellänge von n Bit mit $n \in [2000,3000]$ zulässig. Nach Ende 2023 sind nur noch Schlüssellängen von n mit mehr als 3000 Bit zulässig (vgl. Abschnitt 2.1).

Für den öffentlichen Exponenten e muss gelten

$$2^{16}+1 \leq e \leq 2^{256} \text{ und } ggt(e,\varphi(n))=1$$

[1] PRF(secret, label, seed) = P_MD5(S1, label + seed) XOR P_SHA-1(S2, label + seed);

[2] Die „signature_algorithms“-Extension [RFC-5246, Abschnitt 7.4.1.4.1] fehlt bei TLS Version 1.1.

Für RSA-Signaturen sind folgende Verfahren zulässig:

- RSASSA-PKCS1-v1_5 [PKCS#1] ist genau für folgende Anwendungsfälle bis Ende 2023 zulässig:
  - Für Zertifikatssignaturen von X.509-Zertifikaten und OCSP-Response-Signaturen für diese Zertifikate
  - Für die Verwendung innerhalb von TLS (Authentisierung (Signatur) der ephemeren (EC)DH-Schlüssel, vgl. Abschnitt 4.5.2 bei „Verfahren TLS“)
  - Analog für IKEv2. Es wird empfohlen auf RSASSA-PSS zu migrieren (vgl. [RFC-7427, A.4.3]).
- RSASSA-PSS [PKCS#1] zulässig bis Ende 2024+

Die Verfahren DS2 und DS3 aus [ISO-9796-2] werden aktuell in der TI nicht verwendet.

Für RSA-Verschlüsselung sind folgende Verfahren zulässig:

- RSAES-OAEP [PKCS#1] zulässig bis Ende 2024+

Bei Verwendung von Verfahren, die einen zufälligen Salt-Wert verwenden (bspw. RSASSA-PSS), wird empfohlen die Salt-Länge entsprechend der Länge der Hashfunktion der Mask-Generation-Function zu wählen.

3.3 Verfahren basierend auf dem DL-Problem auf GF(p)

Bei der Schlüsselaushandlung innerhalb von IKEv2 (IPsec) [gemSpec_Krypt, Abschnitt 3.3.1] und bei einigen innerhalb von TLS verwendeten Ciphersuiten [gemSpec_Krypt, Abschnitt 3.3.2] wird ein ephemerer Diffie-Hellmann-Schlüsselaustausch innerhalb von Gruppe 14 [RFC-3526] verwendet. Dies ist, analog zu RSA mit n größer 2000 Bit (vgl. Abschnitt 3.2), bis Ende 2023 zulässig. Nach Ende 2023 wird der Übergang auf die Verwendung eines ephemeren EC-DH entsprechend Abschnitt 3.4 empfohlen.

Aktuell werden in der TI keine weiteren Verfahren, die auf dem DL-Problem auf GF(p) basieren, wie bspw. DSA oder DLIES, in der TI eingesetzt.

3.4 Verfahren basierend auf dem DL-Problem auf elliptischen Kurven

Bei der Verwendung von Verfahren, die auf dem diskreten Logarithmus-Problem auf elliptischen Kurven basieren, wie bspw. ECDSA, ECIES oder (ephemerer) ECDH, sind folgende Kurvenparameter zulässig:

- brainpoolP256r1, brainpoolP384r1 und brainpoolP512r1 [ECCBP] zulässig bis Ende 2024+
- P-256, P-384, P-521 [FIPS-186-4] zulässig bis Ende 2024+

Für eine Schlüsselaushandlungen über EC-DH sind o. g. Gruppen (bzw. Kurvenparameter) bis Ende 2024+ zulässig.

Für Signaturerzeugung und -prüfung ist der Algorithmus ECDSA [FIPS-186-4] bis Ende 2024+ zulässig. Dabei sollte die Bitlänge der verwendeten Hashwerte gemäß [TR-03111] gleich der Bitlänge der Ordnung q der Punktegruppe sein, anderenfalls muss der Hashwert standardkonform abgeschnitten werden (vgl. [TR-03111, Abschnitt 4.2]).

Für Verschlüsselungsverfahren sind ECIES [SEG-1v2] und Verfahren aus [TR-03111, Abschnitt 4.3] jeweils bis Ende 2024+ zulässig.

Für die Anwendung von elliptischen Kurven wird auch auf die Dokumente [TR-03111] und [ECCBP] verwiesen.

3.5 Instanzauthentisierung und Schlüsselvereinbarung

Unter kryptographischer Instanzauthentisierung wird im Folgenden die Authentisierung einer technischen Komponente (Beweisender) als Nachweis einer angegebenen Identität (Identifizierung) gegenüber einer anderen technischen Komponente (Prüfender) durch ein kryptographisches Protokoll verstanden. Der Beweisende weist dabei die Kenntnis (oder allgemeiner die Fähigkeit zur Anwendung) eines Geheimnisses (Verifikationsdaten) nach. Bei symmetrischen kryptographischen Primitiven ist dies ein geheimer kryptographischer Schlüssel und bei asymmetrischen kryptographischen Primitiven ein privater kryptographischer Schlüssel (Verifikationsdaten). Der Prüfende nutzt bei symmetrischen kryptographischen Primitiven den gleichen geheimen kryptographischen Schlüssel und bei asymmetrischen kryptographischen Primitiven einen zum privaten kryptographischen Schlüssel passenden öffentlichen Schlüssel (Referenzdaten). Die Authentisierung kann auch gegenseitig erfolgen.

Zweckmäßigerweise wird die Instanzauthentisierung mit der Vereinbarung geheimer kryptographischer Schlüssel verbunden, um die Vertraulichkeit und Integrität einer anschließenden Kommunikation zwischen den Komponenten zu sichern.

Die Authentisierung mit Chipkarten nutzt die Authentisierung durch Wissen (z. B. PIN) gegenüber der Chipkarte, die danach eine kryptographische Instanzauthentisierung z. B. gegenüber einem Server durchführen kann.

Das PACE-Protokoll verbindet die Authentisierung von Personen mit PIN bzw. Passwort gegenüber einer Chipkarte mit der gegenseitigen Authentisierung und der Vereinbarung von symmetrischen Schlüsseln zwischen dem benutzten Kartenterminal und der Chipkarte zur Verschlüsselung und Datenintegritätssicherung der Kommunikation (siehe Secure Messaging im Kapitel 4.5.2). Es verbindet somit die Benutzerauthentisierung und die Instanzauthentisierung.

3.5.1 Protokolle mit symmetrischen Kryptoalgorithmen

Für den Einsatz in der Telematik im Gesundheitswesen werden grundsätzlich die folgenden symmetrischen Kryptoalgorithmen für Protokolle zur Instanzauthentisierung ggf. mit Aushandlung von kryptographischen Schlüsseln als geeignet bewertet:

- AES-*k* mit k∈{128,192,256} [FIPS-197]

Die Anwendung des AES erfolgt gemäß [FIPS-197].

Das Protokoll zur Authentisierung von Chipkarten gemäß [EN-14890-1, Abschnitt 8.8] und die Ableitung der Sessionkeys auf Grundlage von [ANSI-X9.62, Abschnitt 5.6.3] sind geeignet. Zur Ableitung von Sessionkeys ist eine hierzu geeignete Hashfunktion (siehe Abschnitt 3.2.1) einzusetzen.

3.5.2 Protokolle mit asymmetrischen Kryptoalgorithmen

Für den Einsatz in der Telematik im Gesundheitswesen werden grundsätzlich die folgenden asymmetrischen Verfahren zur Instanzauthentisierung ggf. mit Aushandlung von kryptographischen Schlüsseln als geeignet bewertet:

- RSA Geräteauthentisierung gemäß [eGK Teil1, Abschnitt 16.4.2] und Schlüsselvereinbarung gemäß [eGK Teil 1, Abschnitt 7.2.1],
- Diffie-Hellman-Schlüsselvereinbarung mit Authentisierung gemäß [EN-14890-1, Anhang A.3.1.2],
- PACE gemäß [TR-03110] mit ECDH und AES.

Als grundlegende Algorithmen werden RSA und DSA-Varianten auf elliptischen Kurven als geeignet bewertet. Wenn die gegenseitige Authentisierung von Komponenten mit Schlüsselvereinbarung mit TLS gemäß [RFC-4346] (TLS Version 1.1), [RFC-5246] (TLS Version 1.2) oder mit dem Internet Key Exchange IKEv2 gemäß [RFC-7296] erfolgen soll, sind nur Kryptoalgorithmen, die durch die vorliegende TR-03116-1 als zulässig erklärt werden, zu verwenden. Anwendungsspezifische Einschränkungen werden in Kapitel 4 definiert.

3.6 Datenauthentisierung

Unter kryptographischer Datenauthentisierung werden im Folgenden Verfahren verstanden, die eine Prüfung erlauben, ob Daten bei einer Übertragung oder Speicherung verändert wurden. Ein Datensender (Beweisender) erzeugt unter Verwendung eines Geheimnisses (kryptographischer Schlüssel) für die zu authentisierenden Daten eine Prüfsumme. Der Datenempfänger (Prüfender) prüft, ob die vorgelegte Prüfsumme mit dem Geheimnis des angegebenen Beweisenden für die vorgelegten Daten erzeugt wurden. Bei symmetrischer Datenauthentisierung benutzen Beweisender und Prüfender das gleiche Geheimnis. In diesem Fall kann also auch nicht zwischen dem Beweisenden und dem Prüfenden als möglichem Erzeuger der Prüfsumme gegenüber einem Dritten unterschieden werden. Bei asymmetrischen Verfahren benutzt der Beweisende seinen privaten Schlüssel zur Erzeugung der Prüfsumme und der Prüfende den dazugehörigen öffentlichen Schlüssel zur Prüfung der Daten und der Prüfsumme. Die Zuordnung des öffentlichen Schlüssels zum Besitzer des dazugehörigen privaten Schlüssels erfolgt durch ein Zertifikat.

3.6.1 Hashfunktionen

Eine Hashfunktion berechnet aus einer beliebigen endlichen Zeichenkette eine binäre Folge einer festen Länge (Hashwert). Die wichtigste Eigenschaften kryptographischer Hashfunktionen sind folgend aufgelistet:

- Kollisionsresistenz: Es soll praktisch unmöglich sein, zwei verschiedene Nachrichten zu finden, die den gleichen Hashwert haben.
- Preimage-Resistenz: Zu einem gegebenen zufälligen Hashwert soll es praktisch unmöglich sein, eine Nachricht mit diesem Hashwert zu konstruieren.
- Second-Preimage-Resistenz: Zu einer gegebenen Nachricht soll es praktisch unmöglich sein, eine andere zweite Nachricht zu finden, die den gleichen Hashwert hat.
- Für verschiedene Anwendungen von Hashfunktionen wird oft verlangt, dass die Hashfunktion - beziehungsweise genauer gesagt ein abgeleitetes schlüsselabhängiges kryptographisches Konstrukt wie ein HMAC, der die Hashfunktion als kryptographische Kernkomponente verwendet - nicht unterscheidbar sein soll von einer Zufallsfunktion.

Die Kollisionsresistenz ist unter diesen Eigenschaften den größten praktischen Bedrohungen ausgesetzt.

Für den Einsatz in der Telematik im Gesundheitswesen werden grundsätzlich die Hashfunktionen aus Abschnitt 3.1 als geeignet bewertet.

Derzeit wird der SHA-1 ([FIPS-180-4] und [ISO10118-3]) für den Einsatz in den Verfahren HMAC, Schlüsselableitung und Erzeugung von Zufallszahlen auch noch längerfristig als geeignet bewertet. Allerdings sollten auch für diese Anwendungen, wenn immer möglich, die Hashfunktionen SHA-256, SHA-384, SHA-512 genutzt werden.

3.6.2 Message Authentication Code

Ein Message Authentication Code (MAC) ist ein symmetrisches Datenauthentisierungsverfahren, das sich üblicherweise auf Blockchiffrieralgorithmen und Hashfunktionen als kryptographische Primitive stützt.

Für den Einsatz in der Telematik im Gesundheitswesen werden die folgenden Verfahren zur Erzeugung und Prüfung von Message Authentication Codes als grundsätzlich geeignet bewertet:

- AES-*k* mit k∈{128,192,256} [FIPS-197] innerhalb des CMAC [SP800-38B]
- HMAC-SHA-1 [RFC-2104] bzw. [RFC-2404] mit einer Schlüssellänge von mind. 16 Bytes und mit der Hashfunktion SHA-1 [FIPS-180-4] und [ISO10118-3]
- HMAC-SHA256, -SHA-384, -SHA-512 [RFC-2104] mit einer Schlüssellänge von mind. 16 Bytes und mit den Hashfunktionen SHA-256, SHA-384, SHA-512 [FIPS-180-4]

Die Anwendung des AES erfolgt gemäß [FIPS-197] und CMAC gemäß [SP800-38B]. Bei Verwendung eines CMACs mit einer MAC-Länge kleiner als 128 Bit, ist zu begründen, warum die MAC-Länge im konkreten Anwendungsfall vertretbar ist (vgl. [SP800-38B, Appendix A]).

Das Verfahren HMAC-SHA-1 gilt als geeignet für das in TLS und IKE verwendete Verfahren HMAC. Darüber hinaus kann auch eine der Hashfunktionen aus Abschnitt 3.1 verwendet werden. Gegenüber dem HMAC-SHA1 sind die auf den dort aufgeführten Hashfunktionen basierenden HMAC-Konstruktionen aus Sicherheitssicht vorzuziehen.

3.6.3 Signaturalgorithmen

Für den Einsatz in der Telematik im Gesundheitswesen werden grundsätzlich die Algorithmen für digitale Signaturen, d. h. elektronische Signaturen auf Basis von asymmetrischen Kryptographieverfahren (bspw. RSA, ECDSA), aus Abschnitt 3.2 und 3.4 als geeignet bewertet.

3.7 Verschlüsselung

Die Verschlüsselung dient der Gewährleistung der Vertraulichkeit von Informationen unter der Bedingung, dass Unbefugte die verschlüsselten Daten zur Kenntnis erhalten und nur der Entschlüsselungsschlüssel geheim gehalten wird. Die Integrität der Daten wird allein durch Verschlüsselung nicht geschützt. Die verwendeten Verschlüsselungsverfahren werden für den hier betrachteten Einsatzbereich als bekannt vorausgesetzt. Verschlüsselungsverfahren werden bei der Datenübertragung und der Datenspeicherung eingesetzt.

3.7.1 Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung erfolgt die Verschlüsselung und die Entschlüsselung mit dem gleichen geheimen Schlüssel.

Für den Einsatz in der Telematik im Gesundheitswesen werden grundsätzlich die folgenden symmetrischen Verfahren zur Verschlüsselung als geeignet bewertet:

- AES-*k* im CBC Mode mit $k \in \{128,192,256\}$,
- AES-*k* im Counter Mode (CTR) mit $k \in \{128,192,256\}$ und
- AES-*k* im Galois/Counter Mode (GCM) mit $k \in \{128,192,256\}$.

Die Anwendung des AES erfolgt gemäß [FIPS-197]. Empfehlungen zu den Betriebsarten finden sich in [SP800-38A] und [SP800-38D].

Bei der Verwendung der empfohlenen Betriebsarten für Blockchiffren sind die Hinweise aus [TR-02102-1, Abschnitt 2.1.2] zu beachten. Insbesondere dürfen sich Zählerstände im Counter-Modus und im GCM-Modus nicht innerhalb einer Schlüsselperiode [SP800-57, Abschnitt 2.1] wiederholen. Im CBC-Modus ist die Verwendung unvorhersagbarer oder verschlüsselter Initialisierungsvektoren wie in [TR-02102-1, Abschnitt B.2] sicherzustellen. Im CBC-Modus

und im Counter-Modus sind noch keine kryptographischen Mechanismen zum Schutz der Integrität übertragener Daten enthalten. Es ist im Allgemeinen notwendig, bei Verwendung dieser Betriebsarten einen Integritätsschutz durch separate kryptographische Mechanismen zu implementieren, zum Beispiel durch einen CMAC oder HMAC über die verschlüsselten Daten. Beim Galois/Counter Mode müssen die Anwendungsvorgaben aus [SP800-38D], insbesondere auf die Wahl des Initialisierungsvektors und die maximale Anzahl der Verschlüsselungen mit dem selben Schlüssel eingehalten werden. Weitere anwendungsbezogene Festlegungen erfolgen im Kapitel 4.

Bei Verwendung des AES im CBC-Modus müssen die zu verschlüsselnden Anwendungsdaten mit einem Padding-Verfahren vor der Verschlüsselung behandelt werden, da im Allgemeinen nicht davon auszugehen ist, dass die Länge der Anwendungsdaten immer ein Vielfaches der Blocklänge der AES-Chiffre ist. Wir gehen aber im Folgenden davon aus, dass die Länge der zu übermittelnden Daten wenigstens immer einer ganzen Anzahl von Bytes entspricht. Außerdem nehmen wir an, dass die Blocklänge der verwendeten Blockchiffre kleiner als 256 Byte ist; da der AES als einzige empfohlene Blockchiffre eine Blocklänge von 16 Byte aufweist, ist dies in der Praxis keine Einschränkung. Folgende Padding-Verfahren sind dann zulässig:

- ISO-Padding (vgl. [ISO-7816-4]): Es werden mindestens ein ’80’-Byte und so viele ‘00’-Bytes an die zu verschlüsselnden Anwendungsdaten angehängt, bis die Länge dieser ergänzten Anwendungsdaten in Byte ein Vielfaches der Blocklänge des Blockchiffrieralgorithmus (16 Byte für AES) ist.
- Padding gemäß [RFC-5652]: Bei einer Blocklänge von b Bytes und einer Nachricht von n Bytes wird mit $b - (n \bmod b)$ Bytes des Wertes $b - (n \bmod b)$ (vorzeichenlose 1-Bytezahlen) aufgefüllt.
- ESP-Padding gemäß [RFC-4303][3]: Das erste Padding-Byte ist ’01’, die folgenden Padding-Bytes bilden eine fortlaufende Folge ’02’, ’03’ … (vorzeichenlose 1-Bytezahlen) bis ein Vielfaches der Blocklänge für den Blockchiffrieralgorithmus (16 Byte für AES) erreicht ist.
- Padding gemäß [XMLEnc]: Bei einer Blocklänge von b Bytes und einer Nachricht von n Bytes werden zunächst b - (n mod b) - 1 zufällige Bytes angehängt und abschließend das Byte mit dem Wert b-(n mod b) angehängt. An die Erzeugung der zufälligen Bytes werden hierbei keine der in Abschnitt 3.4 beschriebenen Anforderungen gestellt.

Bei der Verwendung des CBC-Modus ist darauf zu achten, dass nicht aufgrund von Fehlermeldungen Seitenkanalangriffe ermöglicht werden (siehe bspw. [Vaudenay-2002] und [BreakingXMLEnc]).

[3] RFC 4303 lässt bis zu 255 Padding-Bytes zu.

3.7.2 Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung erfolgt die Verschlüsselung mit dem öffentlichen Schlüssel und die Entschlüsselung mit dem privaten Schlüssel, wobei der private Schlüssel praktisch nicht allein aus dem öffentlichen Schlüssel berechnet werden kann.

Für den Einsatz in der Telematik im Gesundheitswesen werden die Verschlüsselungsverfahren in Abschnitt 3.2 und 3.4 zur Verschlüsselung von Schlüsseln als geeignet bewertet.

Asymmetrische Verschlüsselungen werden im allgemeinen nur zur Verschlüsselung von symmetrischen Schlüsseln (Hybridverschlüsselung) und nicht zur Verschlüsselung von Anwendungsdaten verwendet.

3.8 Erzeugung von Zufallszahlen

Die Erzeugung von Zufallszahlen ist erforderlich für die Erzeugung von

- Challenges in Authentisierungsprotokollen,
- zufälligen Paddingbits bzw. Saltwerten sowie
- kryptographischen Schlüsseln bzw. Systemparametern.

Grundsätzlich können für die Erzeugung von Zufallszahlen physikalische Zufallszahlengeneratoren oder Pseudozufallszahlengeneratoren eingesetzt werden. Entsprechend dem gewählten Generator sind die Anforderungen gemäß [AIS-20] für Pseudozufallszahlengeneratoren und [AIS-31] für physikalische Zufallszahlengeneratoren einzuhalten.

Die Erzeugung von **kryptographischen Schlüsseln und Systemparametern** wird in Kapitel 3.9 behandelt.

Für die Erzeugung einer **Challenge in Authentisierungsprotokollen** und von **zufälligen Padding- und Saltbits** sind die folgenden Anforderungen einzuhalten:

- Ein Pseudozufallszahlengenerator muss mindestens ein DRG.2 [AIS-20] sein. Der Seed muss mindestens 100 Bit Entropie besitzen. Nach Ende 2023 muss der Seed mindestens 120 Bit Entropie besitzen.
- Ein physikalischer Zufallszahlengenerator muss mindestens ein P2-TRNG mit Stärke der Mechanismen „Hoch“ oder ein PTG.2 jeweils im Sinne der AIS 31 [AIS-31] sein. Bei Nutzung von PACE darf als physikalischer Zufallszahlengenerator nur ein PTG.3 im Sinne der AIS 31 [AIS-31] verwendet werden.

3.9 Schlüsselerzeugung

Bei der Schlüsselerzeugung für Sicherheitsverfahren werden Zufallszahlen benötigt, an die entsprechende kryptographische Anforderungen zu stellen sind, um die Sicherheit des Gesamtsystems zu gewährleisten. Für die Schlüsselerzeugung können physikalische Zufallszahlengeneratoren oder Pseudozufallszahlengeneratoren eingesetzt werden.

Pseudozufallszahlengeneratoren für die Erzeugung von Schlüsseln müssen mindestens ein DRG.3 [AIS-20] sein. Physikalische Zufallszahlengeneratoren für die Erzeugung von Schlüsseln müssen mindestens ein PTG.2 [AIS-31] sein. Es wird generell empfohlen, zur Schlüsselerzeugung einen physikalischen Zufallszahlengenerator zu verwenden, der ein PTG.3 [AIS-31] sein sollte.

Für symmetrische Schlüssel muss die Seedlänge mindestens gleich der Schlüssellänge sein und die Entropie des Seeds im Wesentlichen so groß wie seine Länge, derart, dass die Entropie des Schlüssels im Wesentlichen seiner Länge entspricht. Bei der Erzeugung von asymmetrischen Schlüsseln sollte beachtet werden, dass jeder im Laufe der Schlüsselerzeugung erzeugte Zufallswert, mit dessen Kenntnis eine praktische Ermittlung des privaten Schlüssels aus dem öffentlichen Schlüssel möglich wäre, für sich genommen mindestens 100 Bit Entropie besitzen muss (empfohlen mindestens 120 Bit und ab 2023 verpflichtend mindestens 120 Bit, bei hybriden Verschlüsselungsverfahren mindestens so viel Entropie wie der symmetrische Verschlüsselungsschlüssel). Ist die Entropie eines solchen Zufallswertes wesentlich niedriger als seine Bitlänge, dann muss darüber hinaus sichergestellt sein, dass es einem Angreifer praktisch unmöglich ist, wesentliche Teile des Zufallswertes richtig zu ermitteln, ohne diesen ganz zu erraten. Für einen Anwender ausnutzbare Zusammenhänge zwischen verschiedenen solchen Zufallswerten dürfen nicht bestehen, selbst wenn diese durch einen deterministischen Zufallsgenerator aus gemeinsamer Seed-Entropie erzeugt wurden.

3.9.1 Symmetrische Schlüssel

AES

Für den AES sind weder schwache noch semi-schwache Schlüssel bekannt, es gibt keine Einschränkung bei der Schlüsselauswahl (vgl. [FIPS 197, Kapitel 6.2]). Es gelten die Vorgaben gemäß Anfang des Abschnitts 3.9 und für die Schlüsselerzeugung und Schlüsselableitung sind die Empfehlungen aus [SP800-133] zu beachten.

3.9.2 Asymmetrische Schlüssel

Für die Erzeugung von asymmetrischen Schlüsseln werden „kryptographisch sichere“ Zufallszahlen gemäß Abschnitt 3.8 benötigt. Im Weiteren gelten die algorithmenspezifischen Anforderungen gemäß Abschnitt 3.2 und 3.4.

Bei allen DSA-Varianten sollten PTG.3-konforme RNGs verwendet werden. Auf jeden Fall muss gewährleistet sein, dass bei der Erzeugung des für jede Signatur individuell generierten „ephemeral key“ k keine nachweisbaren statistischen Schwächen auftreten.

Generell wird empfohlen, für ECC-Verfahren Standardkurven aus [TR-03111] zu verwenden; konkrete freigegebene Kurven können auch beim BSI erfragt werden. Beim Verfahren ECDSA sollte die Bitlänge der verwendeten Hashwerte gemäß [TR-03111] nicht größer als die Bitlänge der Ordnung q der Punktegruppe sein.

3.10 Schlüsselvereinbarung

Die Protokolle zur Schlüsselvereinbarung wurden im Zusammenhang mit der gegenseitigen Authentisierung von Komponenten einschließlich Schlüsselvereinbarung behandelt (vgl. Abschnitt 3.5).

4 Anwendung kryptographischer Verfahren

4.1 Instanzauthentisierung

4.1.1 Einsatzbereich

In der Telematikinfrastruktur wird die Instanzauthentisierung für die einseitige und gegenseitige Authentisierung von Chipkarten (eGK, HBA, SMC), Kartenterminals, Konnektoren, VPN-Konzentratoren, Intermediäre und Webservices angewandt.

Die Chipkarten implementieren kryptographische Verfahren zur gegenseitigen Authentisierung von Karten (Card-to-Card Authentication) ohne oder mit Aufbau eines sicheren Kanals (s. Abschnitt 4.6.2) zwischen eGK, HBA und SMC. Zur Durchführung der Card-to-Card Authentisierung verfügen die Karten über asymmetrische Schlüssel und CV-Zertifikate (CVC), mit denen die Authentizität der öffentlichen Schlüssel verifiziert werden kann. Die öffentlichen Schlüssel der Wurzelinstanz der CVC-PKI haben eine lange Gültigkeit, die Zertifikate der darunter liegenden Zertifizierungsinstanzen haben eine etwas kürzere Gültigkeit, während die Gültigkeit der CV-Zertifikate von Chipkarten auf den Nutzungszeitraum der jeweiligen Chipkarte begrenzt ist.

Im Falle der Kommunikation einer eGK mit dem Versichertenstammdatendienst (VSDD) oder einem Card Application Management System (CAMS) erfolgt eine gegenseitige Authentisierung der Komponenten mit Schlüsselvereinbarung auf der Grundlage symmetrischer Verfahren. Analog kann auch die Kommunikation zwischen einer HBA und einem CAMS auf Grundlage einer Authentisierung mit symmetrischen Verfahren erfolgen. Die symmetrischen Schlüssel sollen für jede Chipkarte verschieden und auf die Lebensdauer der jeweiligen Chipkarte begrenzt sein. Ersteres kann durch eine Schlüsselgenerierung mit ausreichender Entropie (vgl. Abschnitt 3.9) gewährleistet werden.

Die Chipkarten eGK [eGK Teil 2], [eGK-G2-ObjSys], HBA [HBA-ObjSys] und SMC Typ B [SMC-B-ObjSys] speichern und verwenden private Authentisierungsschlüssel und verfügen über X.509-Zertifikate für die zugehörigen öffentlichen Schlüssel für eine kartengestützte client-seitige Authentisierung anderer technischer Komponenten gegenüber Intermediäre und Webservices. Die Kartenterminals und Konnektoren ihrerseits speichern und verwenden ebenfalls private Authentisierungsschlüssel in Sicherheitsmodulen (SM-K, SM-KT) und verfügen über X.509-Zertifikate für die zugehörigen öffentlichen Schlüssel zur Authentisierung gegenüber Komponenten der TI. VPN-Konzentratoren, Intermediäre und Server zentraler Dienste sollen ihre privaten Authentisierungsschlüssel ebenfalls in Sicherheitsmodulen sicher speichern und verwenden. Die X.509-Zertifikate für die zugehörigen öffentlichen Schlüssel zur Authentisierung gegenüber Chipkarten, dezentralen und zentralen Komponenten werden in einer X.509-PKI verwaltet.

Die öffentlichen Schlüssel der Wurzelinstanz der X.509-PKI und darunter liegender Zertifizierungsinstanzen haben eine sehr lange Gültigkeit, für die ein langfristiger Übergang und eine Migrationsstrategie auf größere Schlüssellängen (3000 Bit RSA, 250 Bit ECDSA) empfohlen wird. Die X.509-Zertifikate müssen kurzfristig sperrbar und deren Gültigkeit online abfragbar sein.

4.1.2 Kryptographische Verfahren

Verfahren: Asymmetrische Authentisierung ohne Schlüsselvereinbarung (technische Komponenten, Anwendung Card-to-Card-Authentisierung):

- Es gelten bez. der Verfahren RSA und ECDSA die kryptographischen Anforderungen aus Abschnitt 3.2 und 3.4.
- Bez. der zu verwendenden Hashfunktion gelten die Vorgaben aus Abschnitt 3.1.
- Nicht nur bei der Erstellung, sondern auch bei der Prüfung digitaler Signaturen muss vom Signaturprüfenden sichergestellt werden, dass die zu prüfende Signatur mit einem nach dieser TR zulässigem Verfahren signiert wurde. Dies schließt jeweils neben der Signatur einer Nachricht selbst die gesamte Zertifikatskette bis zu dem passenden Wurzelzertifikat ein.

Im Rahmen der Authentisierung werden CV-Zertifikate verwendet. Für die Erzeugung (Signatur) der Zertifikate und die in den Zertifikaten bestätigten Schlüssel gelten ebenfalls die Vorgaben aus den drei vorhergehenden Spiegelstrichen.

Verfahren: Asymmetrische Authentisierung mit Schlüsselvereinbarung (Anwendung Card-to-Card-Authentisierung inkl. anschließendem Secure Messaging):

- Es gelten die Anforderungen der drei vorhergehenden Spiegelstriche.
- Im Rahmen der Schlüsselvereinbarung zulässige Hashfunktionen für die Ableitung der symmetrischen Schlüssel (Schlüsselableitungsfunktion gemäß [ANSI-X9.63]): SHA-1, SHA-256, SHA-384, SHA-512 bis Ende 2024+

Verfahren: symmetrische Authentisierung gemäß [EN-14890-1] mit Schlüsselvereinbarung (Card-to-Server-Authentisierung; z.B. CAMS oder VSDD):

- AES-128, AES-192, AES-256: bis Ende 2024+

Verfahren: Client-Server-Authentisierung (Authentisierung einer Chipkarte gegenüber einem Server bzw. Kartenterminal):

- RSA gemäß Abschnitt 3.2
- ECDSA über $E(F_p)$ gemäß Abschnitt 3.4
- PACE [TR-03110]

4.2 Qualifizierte elektronische Signatur

Der elektronische Heilberufsausweis verfügt über die Anwendung DF.QES, mit der die Erzeugung von qualifizierten elektronischen Signaturen (qeS) ermöglicht wird. In der elektronischen Gesundheitskarte ist die Anwendung DF.QES optional.

Es werden durch die TR-03116-1 keine weiteren Vorgaben für die qeS gemacht, die neben den schon gesetzlichen Vorgaben bspw. durch die eIDAS-Verordnung [eIDAS] und deren Durchführungsrechtsakte gelten.

4.3 Digitale nicht-qualifizierte elektronische Signaturen

Die technischen Anforderungen an qualifizierte elektronische Signaturen und Zertifikate (vgl. Kapitel 4.2) sind soweit möglich auch für digitale Signaturen (vgl. 3.6.3), die nicht-qualifizierte elektronische Signaturen sind, bzw. für die zur Authentifizierung dienenden Zertifikate einzuhalten.

Es gelten die Vorgaben aus Abschnitt 3.6.3.

4.4 Verschlüsselung von Dokumenten

4.4.1 Einsatzbereich

In der Telematikinfrastruktur muss die Vertraulichkeit von Dokumenten (oder Dokumentteilen) bei deren Übertragung zwischen dem Konnektor und den Telematikdiensten sowie bei deren Speicherung durch die Telematikdienste gewährleistet werden. Die Verschlüsselung erfolgt durch Hybridverfahren, bei denen die Daten der Dokumente symmetrisch mit Dokumentenschlüsseln verschlüsselt werden und die (asymmetrische) Entschlüsselung der Dokumentenschlüssel durch Chipkarten (eGK, HBA oder SMC) oder Hardwaresicherheitsmodule erfolgt.

Wegen der langfristigen Vertraulichkeit der zu schützenden Dokumente und der Schwierigkeit langfristiger Vorhersagen zur Sicherheit der vorgesehenen Kryptoalgorithmen werden die Sicherheitsaussagen unter der Voraussetzung getroffen, dass

- die vertraulichen Dokumente vor der Übertragung über das Internet verschlüsselt werden,
- die Kommunikationskanäle zur Übermittlung der Dokumente selbst verschlüsselt sind,
- für die Speicherung der vertraulichen Dokumente Verfahren vorzusehen sind, die bei Notwendigkeit eine Umschlüsselung oder Überschlüsselung der Dokumente mit stärkeren kryptographischen Verfahren ermöglichen. Im Rahmen einer Umschlüsselung oder Überschlüsselung müssen die alten Chiffrate sicher gelöscht werden. Überschlüsselung bedeutet hierbei die erneute Verschlüsselung eines bereits verschlüsselten Dokuments. Verglichen mit einer Umschlüsselung hat ein solches Vorgehen den Vorteil, dass auf eine große Anzahl von Dokumenten angewendet werden kann, ohne diese zwischenzeitlich

entschlüsseln zu müssen; es hat den Nachteil, dass das unter dem zu ersetzenden Chiffriersystem genutzte Schlüsselmaterial nach Abschluss des Vorgangs weiterhin vorgehalten werden muss.

4.4.2 Kryptographische Verfahren

Verfahren: Hybridverschlüsselung unter Verwendung von [XMLEnc] oder S/MIME [RFC-5751] bzw. Cryptographic Message Syntax (CMS) [RFC-5652]:

- asymmetrische Verschlüsselung des symmetrischen Dokumentenschlüssels (key transport): gemäß Abschnitt 3.2 und 3.4
- symmetrische Verschlüsselung der Dokumentendaten:
  - AES-256 CBC mit zufälligem Initialisierungsvektor bis Ende 2024+
  - AES-256 GCM mit zufälligem Initialisierungsvektor und Tag-Länge von 128 Bit bis Ende 2024+[4]

    Die Bitlänge des Initialisierungsvektors bei der Verwendung von AES-GCM soll 96-Bit sein. Es wird die Verwendung von AES-256 GCM mit der Tag-Länge von 128 Bit empfohlen und als langfristig geeignet bewertet.

Aufgrund der in der Praxis oft beobachteten Anfälligkeit von Implementierungen gegen Seitenkanalangriffe bei Verwendung des CBC-Modus (vgl. [Vaudenay-2002] und [BreakingXMLEnc]) wird die Verwendung von AES/GCM [SP800-38D] empfohlen.

4.5 Kommunikation

4.5.1 Einsatzbereich

Die Telematikinfrastruktur benutzt kryptographische Verfahren zum Schutz der Vertraulichkeit und der Integrität der zweiseitigen Online-Kommunikation zwischen den Chipkarten, den technischen Komponenten der Telematikinfrastruktur im lokalen Netz der Leistungserbringer (Kartenterminal, Konnektor), zwischen dem Konnektor und dem VPN-Konzentrator, dem Intermediär und gegebenenfalls weiteren Komponenten.

[4] Die Anwendungsvorgaben aus [SP800-38D] insbesondere auf die Wahl des Initialisierungsvektors und die maximale Anzahl der Verschlüsselungen mit dem selben Schlüssel müssen eingehalten werden.

4.5.2 Kryptographische Verfahren

Verfahren: Secure Messaging zwischen Chipkarten (Card-to-Card-Kommunikation bzw. Absicherung der Kommunikation zwischen Karte und Server bzw. Kartenterminal):

- symmetrische Schlüsselvereinbarung nach [EN-14890-1], PACE [TR-03110] und [ANSI-X9.63]: siehe Angaben in Kapitel 4.1.2
- asymmetrische Schlüsselvereinbarung nach [EN14890-1]: siehe Angaben in Kapitel 4.1.2
- Verschlüsselung mittels AES-n CBC mit zufälligem Initialisierungsvektor oder mittels AES-n CTR mit zufälligem Initialwert des Zählers (jeweils mit n=128, 192 oder 256) geeignet bis Ende 2024+.
  Wenn der CBC-Initialisierungsvektor (IV) nicht zufällig gewählt wird oder gewählt werden kann, so muss der Verschlüsselungsalgorithmus durch einen anderen Mechanismus dynamisiert werden (z.B. IV ist ein verschlüsselter[5] Counter bzw. als IV wird (wie bei IPsec) der vorherige Output des verwendeten Blockchiffrieralgorithmus genommen). Der CBC-Initialisierungsvektor darf nicht vorhersagbar werden.
- Integritätsschutz: AES-128 [FIPS-197] innerhalb von CMAC [SP800-38B] geeignet bis Ende 2024+

Bei einer Anwendung des Secure Messaging über offene Netze (z.B. bei einer Card-to Server-Kommunikation) muss die Kommunikation durch zusätzliche Sicherheitsmechanismen zur Wahrung der Vertraulichkeit und Datenauthentizität geschützt werden (z.B. mittels IPsec).

Verfahren: IPsec

Die IPsec-Kommunikation zwischen dem Konnektor und dem VPN-Konzentrator und die TLS-Kommunikation zwischen Konnektor und Fachdiensten dürfen generell nur langfristig geeignete Kryptoalgorithmen gemäß Kapitel 3 verwenden. Für die Parameter und Schlüssellängen gelten generell die Festlegungen wie zur Client-Server-Authentisierung des Kapitels 4.1. Allerdings gilt bis Ende 2020 für die Schlüsselerzeugung: Für die Erzeugung symmetrischer Schlüssel ist die Verwendung eines Pseudozufallszahlengenerators der Klasse K4 mit Stärke der Mechanismen „Hoch“ oder der Klasse DRG.3 gemäß [AIS-20] ausreichend; alternativ genügt eine nachvollziehbare Begründung des Antragstellers, dass das Fehlen der K4-spezifischen Eigenschaft im vorgesehenen Einsatzszenario keine zusätzlichen Sicherheitsrisiken induziert; die Entropie des Seeds muss mindestens gleich der Schlüssellänge sein; es wird empfohlen, dass für die Seedgenerierung bzw. für die Schlüsselgenerierung ein PTG.3 im Sinne der AIS 31 [AIS-31] verwendet wird.

[5] Der IV darf nicht gleich dem Counter gewählt werden.

Empfehlungen für die Verwendung von IKE/IPsec findet man in [TR-02102-3].

Bei der Verwendung von IKE/IPsec muss Forward Secrecy (authentisierte DHE oder ECDHE) gewährleistet werden. Für die Authentisierung (Signatur) der ephemeren (EC)-DH-Parameter muss eine nach Abschnitt 3.1 zulässige Hashfunktion verwendet werden. Es wird empfohlen die IKEv2-Erweiterung nach [RFC 7427] zu verwenden.

Ephemere Schlüssel und Sitzungsschlüssel müssen nach ihrer Verwendung unwiderruflich gelöscht werden. Ephemere bzw. Sitzungsschlüssel dürfen nur für eine Sitzung benutzt werden und dürfen grundsätzlich nicht persistent abgespeichert werden. Dies gilt auch für Ephemeralschlüssel, die für die Authentisierung eines Diffie-Hellman-Schlüsseltausches genutzt werden.

Verfahren: TLS

Empfehlungen für die Verwendung von TLS findet man in [TR-02102-2]. Es dürfen nur Ciphersuiten Verwendung finden, die Forward Secrecy ermöglichen. Vorgaben für ephemere und Sitzungsschlüssel gelten analog zu IPsec. Es wird die komplette Migration von TLS Version 1.1 auf die Version 1.2 angestrebt. Andere Versionen von TLS oder von SSL sind in der TI nicht zulässig. Es wird die Verwendung einer CipherSuite empfohlen, die AES im GCM verwendet.

Für TLS ist die Verwendung des Verfahrens RSASSA-PKCS1-v1_5 weiterhin zulässig (vgl. Abschnitt 3.2). Im Gegensatz zur TLS Version 1.3 gibt[6] es bei Version 1.2 (oder 1.1) keinen im Protokoll festgelegten Weg die Verwendung dieses Signaturverfahren im Rahmen des Verbindungsaufbaus als Teil der gemeinsamen Sitzungsparameter auszuhandeln. Die Unterstützung von RSASSA-PSS wird erst mit TLS Version 1.3 für eine TLS-Implementierung verpflichtend.

4.6 Bestandsanwendungen eGK Generation 1

4.6.1 eGK Generation 1

Wissenschaftliche Entwicklungen im Bereich der Kryptographie und technische Entwicklungen in der IT erfordern eine ständige Weiterentwicklung der Komponenten und der Prozesse der Telematikinfrastruktur. Die aktuell im Feld befindliche elektronische Gesundheitskarte der Generation 1 (eGK G1) wird schrittweise durch Karten der Generation 2 ersetzt. Auch diese Karten werden zukünftig wieder durch Karten einer Folgegeneration ersetzt werden.

Im Folgenden sind verbindliche Vorgaben für kryptographische Verfahren, die im Rahmen der Anwendungsprozesse um die eGK G1 Verwendung finden, aufgeführt. Die Vorgaben

[6] https://tools.ietf.org/html/draft-ietf-tls-tls13-28#section-4.2.3

basieren auf aktuellen Erkenntnissen und Veröffentlichungen bez. der Sicherheit der aufgeführten Verfahren und werden ggf. zukünftig an aktuelle Entwicklungen angepasst.

4.6.2 Kryptographische Verfahren

Verfahren: Verschlüsselung

- 3TDES (Triple-DES (TDEA[7]) mit 168 Bit langem Schlüssel) geeignet bis Ende 2018

Das Verfahren 3TDES ist in [SP-800-67r1] definiert als TDEA Keying Option 1. Der 3TDES (Triple-DES 168 Bit Schlüssel) im CBC-Modus ist in der TI nur für Anwendungen im Rahmen der eGK G1 zulässig (VSDD und CAMS-Anwendungen). Es dürfen nur wesentlich weniger als 2^{32} Nachrichtenblöcke mit dem gleichen Schlüssel bearbeitet werden. Die Verwendung von schwachen sowie von semi-schwachen Schlüsseln als Teilschlüssel eines TDES Schlüssels (siehe z.B. [SP800-67r1, Kapitel 3.4.2]) ist praktisch auszuschließen. Darüber hinaus sind die drei Teilschlüssel unabhängig und zufällig zu wählen, so dass diese praktisch paarweise verschieden sind.

Der 2TDES (Triple-DES mit 112 Bit langem Schlüssel / TDEA Keying Option 2 [SP-800-67r1]) wird als nicht geeignet bewertet.

Verfahren: Integritätsschutz

- Das nichtstandardisierte 3TDES basierte MAC-Verfahren „3TDES - Retail CBC MAC“ mit 168 Bit Schlüssel, das in [eGK Teil 1, Abschnitt 7.6] (bzw. [gemSpec_COS, Abschnitt 6.6.1.1]) beschrieben wird, ist nur analog bis Ende 2018 für Anwendungen der eGK G1 zulässig.

Voraussetzung dabei ist, dass der gemäß [eGK Teil 1] Abschnitt 7.2.1 gemeinsam mit dem MAC-Schlüssel K_{mac} abgeleitete, dort als SSC_{mac} bezeichnete und gemäß Abschnitt 14.2 verwendete IV (Initialisierungsvektor) wie ein weiterer 64-Bit Teilschlüssel behandelt (d.h. mit der erforderlichen Entropie erzeugt und genau wie K_{mac} geheim gehalten) wird und dass maximal 2^{16} Nachrichtenblöcke mit dem gleichen Schlüssel bearbeitet werden.

Verfahren: DS1-Signaturen [ISO-9796-2] unter Verwendung von SHA-256

In [EN-14890-1] wird ein Padding für CV-Zertifikate beschrieben, das dem DS1 aus [ISO 9796-2] entspricht. Das Verfahren hat in bestimmen Einsatzszenarien kryptographische Schwächen [Coron-2009]. Deshalb wird dringend empfohlen, auch für CV-Zertifikate eines der in Abschnitt 3.2 und 3.4 aufgeführten Verfahren zu verwenden. Für CV-Zertifikate mit der DS1-Variante gemäß den Abschnitten 7.6 und 8 [eGK Teil 1] muss bei der Erstellung der

[7] Triple Data Encryption Algorithm

CV-Zertifikate (neben der Verwendung von RSA-Schlüsseln der Länge 2048 Bit und der Hashfunktion SHA-256) folgendes gewährleistet sein:

Die CV-Zertifikate werden beim Kartenherstellungsprozess unmittelbar nach Generierung des Schlüsselpaars, die von einem Angreifer nicht beeinflusst werden kann, erstellt. Auch die übrigen Felder des Nachrichtenstrings M gemäß (N 005500) und (N 006300) in Abschnitt 8 von [eGK Teil 1] können nicht von einem Angreifer beeinflusst werden.

Das Verfahren ist im Rahmen der Anwendungen der eGK G1 bis Ende 2018 zulässig. Ansonsten ist das Verfahren innerhalb der TI nicht mehr zulässig.

4.7 Hardware-Unterstützung AES (AES-NI)

Seit 2011 gibt es bei verschiedenen Intel- und AMD-Prozessoren eine Befehlssatzerweiterung namens „Advanced Encryption Standard New Instructions“ (AES-NI)[8] und eine Befehlssatzerweiterungen für die übertragsfreie Multiplikation[9]. Diese ermöglichen im Zusammenspiel eine je nach Anwendungsfall drei- bis zehnfache Beschleunigung der AES-Ausführung im Vergleich zu einer Softwareimplementierung ohne diese Befehlssatzerweiterungen.[10]

Es ist zulässig, diese Befehlssatzerweiterungen im Rahmen

- der Verwendung des IPsec-Protokolls,
- der Verwendung des TLS-Protokolls und
- der Verwendung der hybriden Ver- bzw. Entschlüsselung bspw. für Dokumente, E-Mail, o. Ä.

in der CPU eines Konnektors zu verwenden.

Es muss einem Administrator eines Konnektors möglich sein bez. der AES-Ausführung zwischen einer im Sinne der Common Criteria geprüften Software-AES-Implementierung und einer im CC-Sinne ungeprüften Hardware-AES-Implementierung (ausschließlich direkt im Intel- oder AMD-basierten Hauptprozessor mit AES-NI-Unterstützung) per Konfigurationseinstellung zu wechseln. Dieser Wechsel darf (1) nur durch einen Administrator vorgenommen werden können und muss (2) jederzeit hin und wieder zurück ad infinitum möglich sein.

---

[8] https://software.intel.com/sites/default/files/article/165683/aes-wp-2012-09-22-v01.pdf

[9] PCLMULQDQ, https://de.wikipedia.org/wiki/CLMUL

[10] https://software.intel.com/sites/default/files/article/165683/aes-wp-2012-09-22-v01.pdf

Die spezifischen Vorgaben zu den Anwendungsfällen (vgl. Abschnitt 4) bspw. den für die AES-Verwendung zulässigen Betriebsmodus (bspw. AES/GCM) gelten mit und ohne Verwendung der Befehlssatzerweiterungen.

5 Literatur

[AIS-20] AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.pdf?__blob=publicationFile

[AIS-31] AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_pdf.pdf?__blob=publicationFile

[ANSI-X9.62] American National Standard X9.62 – 2005, Public Key Cryptography for the Financial Service Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005 (ersetzt ANSI X9.62-1998)

[ANSI-X9.63] American National Standard X9.63 – 2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2001

[Coron-2009] Practical Cryptanalysis of ISO/IEC 9796-2 and EMV Signatures, Jean-Sebastien Coron and David Naccache and Mehdi Tibouchi and Ralf-Philipp Weinmann, 2009, https://eprint.iacr.org/2009/203

[BreakingXMLEnc] How to Break XML Encryption, Tibor Jager, Juraj Somorovsky, 2011, http://www.nds.rub.de/media/nds/veroeffentlichungen/2011/10/22/HowToBreakXMLenc.pdf

[ECCBP] ECC Brainpool: Standard Curves and Curve Generation, Vers. 1.0, 2005; online http://www.teletrust.de/fileadmin/files/oid/oid_ECC-Brainpool-Standard-curves-V1.pdf, siehe auch [RFC 5639]

[eGK-G2-ObjSys] Spezifikation der elektronischen Gesundheitskarte, https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/

[eGK Teil 1] Spezifikation der elektronischen Gesundheitskarte, Teil I: Spezifikation der elektrischen Schnittstelle, Version 2.2.0, 20.03.2008, https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/

[eGK Teil 2] Spezifikation der elektronischen Gesundheitskarte, Teil II: Grundlegende Applikationen, Version 2.2.0, 25.03.2008, https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/

[eIDAS] Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Auf-hebung der Richtlinie 1999/93/EG

[EN-14890-1] DIN EN 14890-1:2008, Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services

[FIPS-180-4] FIPS Publication 180-4: Secure Hash Standard (SHS), Federal Information Processing Standards Publication 180-4, U.S. Department of Commerce / NIST, National Technical Information Service, March 2012

[FIPS-186-4] FIPS Publication 186-4: Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, U.S. Department of Commerce / NIST, National Technical Information Service, July 2013

[FIPS-197] FIPS Publication 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, U.S. Department of Commerce / NIST, National Technical Information Service, November 2001

[FIPS-202] NIST, FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, 2015, http://nvlpubs.nist.gov/nistpubs/fips/NIST.FIPS.202.pdf

[gemSiKo] Übergreifendes Sicherheitskonzept der Telematikinfrastruktur, Version 2.3.0 vom 17.07.2008, www.gematik.de

[gemSpec_COS] Spezifikation des Card Operating System (COS), https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/

[gemSpec_Kon] Konnektorspezifikation, https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/

[gemSpec_Krypt] Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/

[HBA-ObjSys] Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem, https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/

[ISO-7816-4] ISO 7816-4: Identification Cards – Integrated Circuit(s) Cards, Part 4: Organization, security and commands for interchange, 2005

[SP800-38A] NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2001 Edition

[ISO10118-3] ISO 10118-3, Information technology – Security techniques – Hash functions, Part 3: Dedicated hash functions, 2nd ed., 2004

[Lenstra 2000] Lenstra, A.K.; Verheul, E.R.: Selecting Cryptographic Key Sizes, PKC 2000, p 446-465, Januar 2000

[Lenstra 2004] Lenstra, A.K.: Key Lengths, Contribution to The Handbook of Information Security, 30. Juni 2004

[PKCS#1] PKCS #1 v2.2: RSA Cryptography Standard, RSA Laboratories, 27.10.2012, vgl. auch https://tools.ietf.org/html/rfc8017

[RFC-2104] Krawczyk, H., Bellare, M., Canetti, R.: HMAC: Keyed-Hashing for Message Authentication, February 1997

[RFC-2404] Madson, C.; Glenn, R.: The Use of HMAC-SHA-1-96 within ESP and AH, RFC 2404, November 1998

[RFC-3526] Kivinen, T.; Kojo, M.: More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE), RFC 3526, May 2003

[RFC-4303] S. Kent: IP Encapsulating Security Payload (ESP), RFC 4303, December 2005

[RFC-4346] Dierks, S.; E. Rescorla: The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006

[RFC-5246] Dierks, S.; E. Rescorla.: The TLS Protocol, RFC 2246, Version 1.2, August 2008

[RFC-5639] M. Lochter, J. Merkle: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010

[RFC-5652] R. Housley: Cryptographic Message Syntax (CMS), RFC 5652, September 2009

[RFC-5751] B. Ramsdell, S. Turner: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2, January 2010, https://tools.ietf.org/html/rfc5751

[RFC-7296] C. Kaufmanm, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen: Internet Key Exchange Protocol Version 2 (IKEv2), October 2014, https://tools.ietf.org/html/rfc7296

[RFC-7427] T. Kivinen, J. Snyder: Signature Authentication in the Internet Key Exchange Version 2 (IKEv2), January 2015, https://tools.ietf.org/html/rfc7427

[RSA] R. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, Vol. 21 No. 2, 1978

[SMC-B-ObjSys] Spezifikation der Security Module Card SMC-B Objektsystem, https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/

[SOGIS-2018] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.1 June 2018, http://www.sogisportal.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.1.pdf

[SP800-38A] NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2001 Edition

[SP800-38A] NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2001 Edition (Updated 10/6/2016)

[SP800-38D] NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, National Institute of Standards and Technology, U.S. Department of Commerce, November 2007

[SP800-67r1] NIST Special Publication 800-67 Revision 1: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revised January 2012, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, January 2012

[SP800-133] NIST Special Publication 800-133: Recommendation for Cryptographic National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Dezember 2012

[Stevens-2017] The first collision for full SHA-1, Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, Yarik Markov, February 2017, https://eprint.iacr.org/2017/190

[TR-02102-1] Technische Richtlinie BSI TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version: 2018-02, Stand 29. Mai 2018

[TR-02102-2] Technische Richtlinie TR-02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version: 2018-01

[TR-02102-3] Technische Richtlinie TR-02102-3, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Version: 2018-01

[TR-03110] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2 – Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE),and Restricted Identification (RI), Version 2.11, 21.12.2016.

[TR-03111] BSI. Technical Guideline: Elliptic Curve Cryptography, TR-03111, Version 2.10, 2018-06-01.

[TR-03116-2] Technische Richtlinie TR-03116-2, eCard-Projekte der Bundesregierung, Teil 2 – Hoheitliche Ausweisdokumente, Stand: 2018, Datum: 23. April 2018

[TR-03116-3] Technische Richtlinie TR-03116-3 eCard-Projekte der Bundesregierung, Teil 3 – Intelligente Messsysteme, 2018, Datum: 23. April 2018

[TR-03116-4] Technische Richtlinie TR-03116-4, eCard Projekte der Bundesregierung, Teil 4 – Kommunikationsverfahren im eGovernment, Stand: 2018, Datum: 23. April 2018

[TR-03116-5] Technische Richtlinie TR-03116-5, eCard Projekte der Bundesregierung, Teil 4 – 5: Anwendungen der Secure Element API, Stand: 2018, Datum: 6. Juni 2018

[Vaudenay-2002] Security Flaws Induced by CBC Padding: Applications to SSL, IPsec, WTLS … , Serge Vaudenay, Eurocrypt 2002, LNCS 2332/2002, 535-545

[XMLEnc] XML Encryption Syntax and Processing Version 1.1, W3C Recommendation, 11 April 2013, http://www.w3.org/TR/xmlenc-core1/

[XMLDSig] XML Signature Syntax and Processing (Second Edition), W3C Recommendation, 11 April 2013, http://www.w3.org/TR/xmldsig-core1/